COMMENT

NEW LEGAL PROBLEMS, OLD LEGAL SOLUTIONS: BAILMENT THEORY AS THE BASELINE DATA SECURITY STANDARD OF CARE OWED TO AN OPPONENT'S DATA IN E-DISCOVERY

WILLIAM LAROSA†

INTRODUCTION

The discovery process involves the transfer of relevant and responsive information in litigation or government investigations from a producing party to a receiving party. Generally, the information that is transferred has

† J.D. Candidate, University of Pennsylvania Law School, 2019; B.A., Lafayette College, 2016. I would like to thank Professor David Kessler for his constant guidance in helping me develop the theories and arguments in this Comment. I am also grateful to the editors of the University of Pennsylvania Law Review for their commitment and incredibly hard work.

been extensively culled and distilled through the discovery process into a set of refined, relevant data. This data is at an extremely high risk of containing information that is proprietary, trade secret, commercially sensitive, or potentially embarrassing.[1]

In traditional discovery, the biggest risk to parties' data came from misuse by the opposing party.[2] Unlike traditional discovery, however, discovery in modern complex litigation has become primarily electronic.[3] The digitization of discovery has created new data security threats to parties' proprietary data from third parties. The transfer of electronically stored information ("ESI"), in any instance, is antithetical to data security. As a general rule, "less data in fewer places is less vulnerable. In cases of sensitive information, the most powerful security measure remains nondisclosure."[4] But absent undue burden or cost, a party litigating in federal court is presumptively entitled to relevant information in the possession, custody, or control of their opponent.[5] Without adequate security measures in place, the sensitive data that is produced in discovery is placed at risk of cyber-attacks[6] or corporate espionage that may severely injure the producing party.[7]

---

1 *See, e.g.*, Kenneth C. Johnston & Dan Klein, *The February 2016 California Attorney General's Data Breach Report Sets A Standard for "Reasonable Security"—What Does This Mean for Cybersecurity Litigation?*, BUS. L. TODAY, May 2016, at 1-2 (discussing various types of information held by businesses and highlighting the consequences of data security breach); *see also* Richard P. Campbell, *The Protective Order in Products Liability Litigation: Safeguard or Misnomer?*, 31 B.C. L. REV. 771, 773 (1990) (noting the importance of protective orders to shelter parties who otherwise would be required to respond to discovery requests from invasion of privacy by plaintiffs, the public, and the press).

2 David J. Kessler, Jami Mills Vibbert & Alex Altman, *Protective Orders in the Age of Hacking*, N.Y.L.J., Mar. 16, 2015, at 1.

3 *See* Matthew M. Neumeier, Brian D. Hansen & Irina Y. Dmitrieva, *Paper Or Plastic?—The Hunt for Electronic Treasure During Discovery*, JENNER & BLOCK (Dec. 2003), https://www.lexisnexis.com/applieddiscovery/lawlibrary/whitePapers/ADI_Mealeys_PaperPlastic.pdf [https://perma.cc/J3TY-M7VH] (describing how "[e]lectronic information and communications have firmly entrenched themselves in the modern business world").

4 *Id.* at *3.

5 *See generally* FED. R. CIV. P. 34(a); FED. R. CIV. P. 26(b).

6 Law firms are specifically targeted by hackers at an alarmingly high rate. *See* Susan Hansen, *Cyber Attacks Upend Attorney-Client Privilege*, BLOOMBERG BUSINESSWEEK (Mar. 19, 2015, 2:56 PM), http://www.bloomberg.com/news/articles/2015-03-19/cyber-attacks-force-law-firms-to-improve-data-security [https://perma.cc/H5GS-XGML] ("[A]t least 80 of the 100 biggest firms in the country . . . have been hacked since 2011."); Ellen Rosen, *Hackers Seek Corporate Secrets, Breach Big Law Firms*, BLOOMBERG BNA (Mar. 25, 2015), http://www.bna.com/hackers-seek-corporate-n17179924553/ [https://perma.cc/AP3B-HUAN] (noting that "most big law firms have . . . been hacked").

7 *See* Kessler et al., *supra* note 2, at 2 ("A nonparty competitor, for example, could engage in cyber espionage and reap a treasure trove of trade secrets. Cyber terrorists can virtually hold an entire company hostage . . . .").

Although a party may institute its own data security protections to defend from these rising threats,[8] it cannot directly control the conduct of its opponents, their lawyers, or their vendors. Traditionally, courts have not articulated a specific duty, or incentive, for opposing parties to adequately protect their opponent's data, and have relied on protective orders to remedy this malincentive and gap in the law.[9] In federal court, a judge may "issue an order to protect a person from annoyance, embarrassment, oppression, or undue burden or expense."[10] The traditional use of a protective order shielded parties from intentional misuse of data by their opponent.[11] But protective orders may also include provisions designed to ensure that adequate data security measures are put in place to protect data from third party attacks while stored by the opposing party.[12] Some protective orders set forth remedial measures for instances where there is a data breach.[13]

The real issues on the duty to protect an opponent's data arise when there is no protective order in place, or during the negotiations of such protective orders. Some discovery litigation has raised questions of the receiving party's obligations to protect the data of the producing party when there is no protective order. In *Seattle Times Co. v. Rhinehart*,[14] the Supreme Court held that a protective order may prohibit the dissemination of information obtained in discovery to the press without violating the First Amendment,[15] but did not declare whether there is a baseline obligation that prevents an opposing party from disclosing information learned through the discovery process to the press. Absent a protective order, it is unclear under *Seattle Times* what legal duty, if any, is owed by a receiving party.

---

8 For a full discussion of recommended data security measures, see THE SEDONA CONFERENCE, THE SEDONA CONFERENCE INTERNATIONAL PRINCIPLES: DISCOVERY, DISCLOSURE & DATA PROTECTION IN CIVIL LITIGATION (Transitional Ed. Jan. 2017).

9 *See generally* Donald J. Rendall, Jr., *Protective Orders Prohibiting Dissemination of Discovery Information: The First Amendment and Good Cause,* 1980 DUKE L.J. 766, 770 (1980).

10 FED. R. CIV. P. 26(c).

11 *See, e.g.*, Rendall, *supra* note 9, at 771 (describing how the protective order mechanism "satisfies the liberal disclosure policies underlying the discovery process" and simultaneously "minimizes the harm to the producing party from the release of the confidential information").

12 *See, e.g.*, *Model Protective Order*, S.D. CAL. 1, 7, https://www.casd.uscourts.gov/Attorneys/Lists/Forms/Attachments/68/Model%20Protective%20Order.pdf [https://perma.cc/9S9Q-43UD] (providing standard protective order provisions for federal court that require the receiving party to protect confidential and sensitive information of the producing party, as well as provisions that require the deletion or return of the sensitive data at the end of litigation).

13 The Sedona Conference has addressed the need for data security provisions in protective orders as a means of meeting international requirements of cross-border data protection. *See* THE SEDONA CONFERENCE, *supra* note 8, at Appendix C (recommending a Model U.S. Federal Court Protective Order that includes remedial measures for instances when a data breach occurs.)

14 467 U.S. 20 (1984).

15 *Id.* at 33.

In a paper world, this issue was trivial. Standard security protocols like a lock and key were sufficient protective measures to secure paper documents. But, in an electronic data world, this question has become anything but trivial. The value of information stored in an electronic format has increased dramatically.[16] There is now a pressing need for new security protocols and affirmative guidance under the law.

This Comment suggests a baseline standard of care that should be owed by a receiving party in discovery to protect the electronic data of the producing party. Where immense value is present in stored data, the receiving party's duty of care to protect that data is of utmost importance. Establishing a baseline duty of care will provide certainty under the law and will play an essential role in future discovery negotiations.

One major benefit to setting a clear legal standard is certainty.[17] The discovery world is guided by reasonableness. According to Federal Rule 26(b)(1), discovery is only permitted when it is reasonable.[18] Courts have the power to provide some clarity to the vague reasonableness standard by explicitly stating what a receiving parties' legal obligation is under the law to protect their opponent's data. Clarifying the legal standard would provide parties with some guidance as to what security measures are reasonable. Absent action by courts, legislation or regulation may specify a reasonable electronic security standard.[19] Outside of the discovery context, some states, including California and Texas, have introduced regulatory regimes requiring that businesses provide reasonable data security measures to protect customers' personal information.[20] In the absence of government action, however, the courts may set forth a common-law baseline to guide the discovery world.

A clear baseline standard of care will also allow parties to effectively negotiate an agreement over what provisions to include in a protective order to ensure data security. The discovery process is often the most expensive part of litigation.[21] Yet implementing effective data security provisions entails

---

16 *See* Richard K. Herrmann, Vincent J. Poppiti & David K. Sheppard, *Managing Discovery in the Digital Age: A Guide to Electronic Discovery in the District of Delaware*, 8 DEL. L. REV. 75, 75 (2005) ("We are no longer satisfied with discovering documents from the file cabinets of our adversaries. As technology increases, fewer and fewer documents are reduced to paper. Indeed, current statistics indicated that 93% of all documents in the United States are created electronically.").

17 *See, e.g.*, Liong Lim, *Approaches to Liability for Breaches in Data Security*, 3 MACARTHUR L. REV., 81, 96 (1999) (listing certainty as a key element to data security law because "[p]arties must be able to know what standards of security are considered reasonable").

18 FED. R. CIV. P. 26(b)(1).

19 *See* Lim, *supra* note 17, at 96 (suggesting that the government "tak[e] the bold step of identifying acceptable electronic security standards").

20 *See, e.g.*, Johnston & Klein, *supra* note 1, at 1.

21 *See* Statement by Lawyers for Civil Justice, Civil Justice Reform Grp. & U.S. Chamber Inst. for Legal Reform, Statement on Litigation Cost Survey of Major Companies, *in* 2010 Conf. on Civ.

numerous considerations and strategies that entail their own costs.[22] Producing parties will want the most extensive security measures in place to protect their sensitive data. Receiving parties will want to spend as little money as is necessary to protect their opponents' data. These misaligned incentives drive and prolong protective order negotiations.[23]

When there is no agreement under the law as to what the default obligations are in discovery, there is no way for parties to know what to concede and where to stand their ground in negotiations about protective order provisions. This Comment calls on courts to set a standard that will provide discovery attorneys with certainty and guide attorneys in future protective order negotiations.

There is no need to reinvent the wheel in setting a standard. Some data security scholars have suggested turning to existing rules on the duty of care in contract law, tort law, criminal law, or property law for setting a data security standard.[24] The best guide to establishing a baseline standard of care owed by a receiving party to protect the producing party's data lies in the property law principle of bailment. A bailment is a legal relationship "created by the delivery of personal property by one person to another in trust for a specific purpose, pursuant to an express or implied contract to fulfill that trust."[25] Importantly, after the specific purpose has been fulfilled, the delivered property is redelivered to the producer, "dealt with according to his directions, or kept until he reclaims it."[26] This Comment asserts that the receiving party gains no ownership interest in information obtained through discovery. Thus, the exchange of electronic data in discovery is akin to the creation of a bailment, and the existing legal standards of bailment should control.

This Comment begins by addressing the lingering questions that were created by the Supreme Court's holding in *Seattle Times Co. v. Rhinehart*.[27] Part II argues that the ownership rights over data do not transfer to the receiving party in discovery. Part III addresses the history of the consideration of

---

Litig. Duke Law Sch. (May 2010) 2 ("[T]he high transaction costs of litigation, and in particular the costs of discovery, threaten to exceed the amount at issue in all but the largest cases.").

22 *See generally* AM. INTELL. PROP. L. ASS'N, SAFE AND SECURE: CYBER SECURITY PRACTICES FOR LAW FIRMS, A CNA PROFESSIONAL COUNSEL GUIDE FOR LAWYERS AND LAW FIRMS 5-8 https://www.cna.com/web/wcm/connect/61aec549-ac28-457b-8626-aa791c782459/Safe_Secure_Cyber_Security_Practices.pdf?MOD=AJPERES [https://perma.cc/2MSC-B7H2] (describing data security costs).

23 Parties often engage in robust negotiations over electronic discovery and protective orders at meet-and-confer conferences. Herrmann et al., *supra* note 16, at 78.

24 *See* Lim, *supra* note 17, at 90-96 (summarizing approaches to data security that span various legal areas).

25 8A AM. JUR. 2D *Bailments* § 1 (2018).

26 19 SAMUEL WILLISTON & RICHARD A. LORD, A TREATISE ON THE LAW OF CONTRACTS § 53:1 (4th ed 2000).

27 467 U.S. 20 (1984).

bailment liability to electronic information in data security breach cases. Key cases such as *Richardson v. DSW, Inc.*,[28] *In re Sony Gaming Networks & Customer Data Security Breach Litigation*,[29] and *In re Target Corp. Data Security Breach Litigation*[30] dealt with the issue of whether electronic data can be personal property that constitutes a bailment. These cases denied the extension of bailment liability to the transfer of electronic data, reasoning that there was no delivery of property that is required for the creation of a bailment. But these cases did not deal directly with the transfer of data in the context of discovery.

Part IV sets the stage for the application of bailment principles to electronic discovery by explaining that electronic data is intangible property that may be bailed. Part V lays out the requirements for the creation of a bailment of electronic data. In Part V, I also argue that the transfer of electronic data in discovery satisfies the elements for the creation of a bailment. Part VI then explains the standard of care that should apply to the receiving party in discovery to protect its opponent's data. Finally, this Comment concludes by reflecting on the impact establishing a baseline standard of care would have on the discovery process.

I. QUESTIONS LINGERING AFTER *SEATTLE TIMES CO. V. RHINEHART*

The Supreme Court's holding in *Seattle Times* raised several key issues that are essential to this analysis. *Seattle Times* dealt with a defamation action after a newspaper published several disparaging articles about the spiritual leader of the Aquarian Foundation, a religious organization.[31] During the discovery process, the Foundation refused to produce its list of donors and members.[32] The trial court ordered the Foundation to produce the information but also issued a protective order which prohibited the Seattle Times "from publishing, disseminating, or using the information in any way except where necessary to prepare for and try the case."[33]

Wishing to publish the list of donors and members of the Foundation in its newspaper, the Seattle Times appealed the protective order.[34] The Supreme Court of Washington upheld the protective order, concluding that the dissemination of the donor information would "result in annoyance, embarrassment and even oppression."[35]

---

28 No. 05-4599, 2005 WL 2978755, at *4 (N.D. Ill. Nov. 3, 2005).

29 903 F. Supp. 2d 942, 974-75 (S.D. Cal. 2012).

30 66 F. Supp. 3d 1154, 1177 (D. Minn. 2014).

31 *Seattle Times*, 467 U.S. at 22.

32 *Id.* at 25.

33 *Id.* at 27.

34 *Id.*

35 *Id.* at 28.

On appeal to the Supreme Court, the appellant Seattle Times argued that First Amendment freedom of the press should effectively trump the protective order.[36] The Supreme Court disagreed.[37] The Court held that a protective order may limit the ways a party can use information obtained through discovery without violating the First Amendment.[38] The Court reasoned that the Seattle Times had no right in the first instance to publish the information obtained in the pretrial discovery process.[39] The Court recognized the danger posed by the dissemination of information obtained in discovery, noting that "[t]here is an opportunity, therefore, for litigants to obtain—incidentally or purposefully—information that not only is irrelevant but if publicly released could be damaging to reputation and privacy."[40]

Seattle Times does not stand for the principle that absent a protective order, a receiving party has no obligation to protect the producing party's documents and information. The primary issue on which the case turned was whether the First Amendment right to freedom of the press superseded the Seattle Times' discovery obligations and the court-ordered protective order.[41] Even if *Seattle Times* stood for the proposition that the receiving party has the right to publish the information absent a protective order, the case certainly does not bestow the right on the receiving party to allow the information it receives in discovery to be stolen. Providing no protections whatsoever to the information received in discovery leaves sensitive data at risk of theft of public dissemination. The *Seattle Times* Court expressed concerns of the dangers posed by dissemination of sensitive information to the public, noting the "significant potential for abuse" that "may seriously implicate privacy interests of litigants and third parties."[42] The notion that *Seattle Times* stands for the principle that there is no obligation on the receiving party to protect this information in the absence of a protective order ignores the express concerns highlighted by the Supreme Court in its opinion. Thus, *Seattle Times* cannot be understood to support this notion.

Discovery is rarely filed in public court.[43] In *Seattle Times*, the newspaper received the donor list—purely private information—legally through the

---

36 *Id.* at 30-31.

37 *Id.* at 36.

38 *Id.*

39 *Id.* at 33.

40 *Id.* at 35.

41 *Id.* at 32.

42 *Id.* at 34-35.

43 *See* Richard L. Marcus, *Myth and Reality in Protective Order Litigation*, 69 CORNELL L. REV. 1, 15 (1983) ("The fruits of discovery are often not filed in court, and, even when they are, the public may not have access to them."). The issues in this paper do not infringe the right to public trials and do not reach the question of precautions that should (or should not) be taken at the time of trial.

judicial process.[44] By its nature, pretrial discovery is an intrusion into a party's private information.[45] The Court noted that "[i]t does not necessarily follow . . . that a litigant has an unrestrained right to disseminate information that has been obtained through pretrial discovery."[46] The Seattle Times could not claim that there was a First Amendment violation when they never had an ownership interest in this information to begin with.

Seattle Times established that a protective order that satisfies the "good cause" requirement of Rule 26(c) may be issued without offending the First Amendment.[47] But the court left several key questions unanswered. When there is no protective order in place, what duty is owed by the receiving party to protect the information of the producing party? Are there any limits on a receiving party's use of information acquired in discovery from the producing party? Had the protective order not been granted, would the Seattle Times have been free to do whatever it wished with the information obtained in discovery?

One of the most important lingering questions is whether the producing party retains an exclusive ownership interest over the information transferred in discovery. The exclusive ownership interest is a prerequisite for a successful theory of bailment.[48] One may make the reasonable inference from the *Seattle Times* holding that the private information obtained through the discovery process does not create an ownership interest in the receiving party. But while the court held that a litigant does not have an unrestrained right to disseminate information, it made no direct ruling on the ownership rights of the producing and receiving parties over the information.

These questions have been left largely unanswered in the thirty-four years since the *Seattle Times* decision. The importance of determining these answers has been amplified in a world increasingly dominated by electronic discovery. This Comment will proceed by determining whether the receiving party obtains an ownership interest in ESI transferred in discovery.

II. OWNERSHIP OF ESI DOES NOT TRANSFER IN DISCOVERY

The production of electronically stored information in discovery does not equate to a transfer of ownership over those documents and data. The ownership of the ESI is retained by the producing party, but a temporary possessory

---

44 *Seattle Times*, 467 U.S. at 32.

45 *See* Andrew D. Goldstein, *Sealing and Revealing: Rethinking the Rules Governing Public Access to Information Generated through Litigation*, 81 CHI. L. REV. 375, 412 (2006) ("Whether or not discovery is presumptively private has a critical impact on what it means for a court to issue a protective order. If the public has a presumptive right to access discovery materials, a Rule 26(c) protective order would restrain not just the parties . . . but also the public.").

46 *Seattle Times*, 467 U.S. at 31.

47 *Id.* at 37.

48 *See supra* note 25–26 and accompanying text.

interest is transferred to the receiving party during the litigation. If the receiving party does not own the data, it is not their data to distribute or to lose.

A copy of ESI that is produced in discovery has a limited purpose and is not for indefinite retention. In discovery, information is not transferred willingly—but on a legal obligation.[49] The receiving party's right to use this data is not unlimited.[50]

The true purpose of the discovery process is to provide parties with the information needed to prove their claims and defenses in litigation "to secure the just, speedy, and inexpensive determination of every action and proceeding."[51] The *Seattle Times* Court noted that the newspaper "gained the information they wish[ed] to disseminate only by virtue of the trial court's discovery processes. . . . A litigant has no First Amendment right of access to information made available only for purposes of trying his suit."[52] The dissemination of confidential information serves no purpose in litigation.[53] Litigation is not indefinite, and neither are the possessory rights of the receiving party over the producing party's information. The majority of courts hold that the information transferred in discovery is not for public access.[54] Rather, the presumption is that the receiving party may use the information obtained through the discovery process *solely* for use in litigation. To obtain the information, the requesting party must first establish that the documents are relevant—that they will assist the parties and the trier of facts to resolve a disputed question of fact.[55]

When considering whether receiving parties obtain an ownership interest in discovery materials, it is instructive to consider the Canadian approach to

---

49 Parties are legally obligated to produce documents and data during the discovery phase of litigation. *See* FED. R. CIV. P. 26(b)(1) ("Parties may obtain discovery regarding any nonprivileged matter that is relevant to any party's claim or defense and proportional to the needs of the case . . . .").

50 *Seattle Times*, 467 U.S. at 31 ("It does not necessarily follow . . . that a litigant has an unrestrained right to disseminate information that has been obtained through pretrial discovery.").

51 FED. R. CIV. P. 1.

52 *Seattle Times*, 467 U.S. at 32.

53 *See* Rendall, *supra* note 9, at 770 n.25 ("[D]iscovery is principally a litigation tool, not a mechanism for forced publication of confidential information. Dissemination of discovery information does not make litigation more efficient, or aid in preparation for trial.")

54 *See, e.g.*, SEC v. TheStreet.com, 273 F.3d 222, 233 (2d Cir. 2001) (stating that information transferred in discovery "do[es] not carry a presumption of public access"); Leucadia, Inc. v. Applied Extrusion Techs., Inc., 998 F.2d 157, 165 (3d Cir. 1993) (denying public access to supporting materials attached to discovery motions); Anderson v. Cryovac, Inc., 805 F.2d 1, 11-12 (1st Cir. 1986) ("We think it is clear and hold that there is no right of public access to documents considered in discovery motions.").

55 FED. R. CIV. P. 26(b)(1); *see also* ADVISORY COMM. ON RULES FOR CIV. PROC., NOTES TO 2015 AMENDMENT OF FED. R. CIV. P. 26(b)(1) ("A party claiming that a request is important to resolve the issues should be able to explain the ways in which the underlying information bears on the issues as that party understands them.").

discovery of the "implied undertaking."[56] The implied undertaking principle prevents litigants from using information obtained in the discovery process for purposes unrelated to the current matter.[57] The implied undertaking binds all parties and counsel in a case.[58]

In a criminal investigation involving child abuse, the Canadian Supreme Court in *Juman v. Doucette* held that the implied undertaking prevented the Attorney General of British Columbia from obtaining discovery transcripts used in a prior civil action against the same defendant.[59] The Canadian Supreme Court provided two rationales for this decision. The first rationale mirrors the concerns expressed by the United States Supreme Court in *Seattle Times*, namely that discovery is an invasion into a litigant's privacy:[60]

> The public interest in getting at the truth in a civil action outweighs the examinee's privacy interest, but the latter is nevertheless entitled to a measure of protection. The answers and documents are compelled by statute solely for the purpose of the civil action and the law thus requires that the invasion of privacy should generally be limited to the level of disclosure necessary to satisfy that purpose and that purpose alone. . . . The general idea, metaphorically speaking, is that *whatever is disclosed in the discovery room stays in the discovery room* unless eventually revealed in the courtroom or disclosed by judicial order.[61]

The second rationale posed by the Canadian Supreme Court was that, absent an understanding that their information would be protected by the implied undertaking, litigants would not have an incentive to "provide a more complete and candid discovery."[62]

Canada's implied undertaking approach provides a solution to the problem discussed in this Comment. There is a baseline duty of protection under Canadian law that has not been expressly articulated under American law.[63]

---

56 Craig Gillespie, The Implied Undertaking in Discovery 1 (unpublished manuscript), http://www.bottomlineresearch.ca/pdf/The%20Implied%20Undertaking%20in%20Discovery.pdf [https://perma.cc/93PG-F2JL].

57 See *id.* (noting that the implied undertaking principle prohibits litigants from "us[ing] information obtained during the discovery process for purposes unrelated to the proceeding").

58 *Id.*

59 Juman v. Doucette, [2008] 1 S.C.R. 157, ¶ 51 (Can.).

60 Seattle Times Co. v. Rhinehart, 467 U.S. 20, 35 (1984).

61 *Doucette*, [2008] 1 S.C.R. 157 at ¶ 25 (emphasis added).

62 *Id.* at ¶ 26.

63 Some litigants have taken advantage of the absence of an implied undertaking in the United States. *See, e.g.*, Barry Leon & Cynthia Tape, *Managing Cross-Border Pharmaceutical Class Actions in Canada*, 15 ANDREWS CORP. CORRUPTION LITIG. REP., July 26, 2004, at *2 (explaining that cross-border pharmaceutical class actions involving the United States and Canada are almost always brought in the U.S., largely because of the absence of an implied undertaking obligation).

The rationales highlighted by the Canadian Supreme Court, however, are just as valid under U.S. common law and U.S. jurisprudence. The same privacy invasions are at stake from public dissemination of private information. And when a protective order is not in place, a producing party is, at minimum, disincentived from making a complete and candid discovery.[64]

The Canadian implied undertaking approach is founded on the fact that a producing party maintains its ownership rights of private information contained in discovery materials.[65] The receiving party obtains a temporary possessory interest in that information for use in litigation. The common understanding in Canada is that property rights over information transferred in discovery are maintained by the producing party. By observing standard protective and confidential order provisions, it is apparent that while there is no present legal baseline, the same understanding of the ownership interests at stake exists in American law.

Protective orders have become increasingly common, but no standard form exists.[66] Yet nearly all protective orders include provisions that require the nondisclosure and destruction of data after litigation.[67] In a boilerplate confidentiality agreement,[68] confidential information may be defined as "any information that a party believes in good faith to be confidential or sensitive information, including, but not limited to, trade secrets, research, design, development, financial, technical, marketing, planning, personal, or commercial information, as such terms are used in Rule 26(c)(1)(G) of the Federal Rules of Civil Procedure . . ."[69] Parties often add provisions expanding their definition of confidential information to expand the scope of the confidentiality agreement. Parties may designate some information as highly confidential, subject to greater protections.[70]

---

64 *See generally infra* Part V (arguing that the production of sensitive data absent a protective order may amount to negligence on the part of counsel).

65 Kandace Terris, *Discovery and the Formulation of the Implied Undertaking Rule in Nova Scotia*, 22 NOVA SCOTIA L. NEWS 137, 144 (1996) http://www.lians.ca/sites/default/files/documents/DiscoveryAndTheFormulation.pdf (noting that the implied undertaking rule "is based on recognition of the general right of privacy of a person respecting his or her documents. Intrusion resulting from discovery should not be allowed for any purpose other than that of securing justice in the proceeding in which the discovery takes place").

66 William Lynch Schaller, *Protecting Trade Secrets During Litigation: Policies and Procedures*, 88 ILL. B.J. 260, 262 (2000).

67 Dustin B. Benham, *Proportionality, Pretrial Confidentiality, and Discovery Sharing*, 71 WASH. & LEE L. REV. 2181, 2189 (2014) (describing confidentiality agreements and protective orders that "often include 'return-or-destroy' provisions that require the parties to return or destroy all discovery information in the case within a few months of settlement").

68 Note that a confidentiality agreement is a private agreement between parties. A protective order, by contrast, is an order of the court that *supersedes* private confidentiality agreements.

69 *See* THE SEDONA CONFERENCE, *supra* note 8, at 40-41.

70 *Id.* at 41.

A standard protective or confidentiality order provision may appear as follows:

> The recipient of any Confidential Material or Highly Confidential Material that is provided under this Protective Order shall maintain such information in a *reasonably secure* and safe manner that ensures that access is limited to the persons authorized under this Order, and shall further exercise the same standard of due and proper care with respect to the storage, custody, use, and/or dissemination of such information as is exercised by the recipient with respect to its own proprietary information.[71]

Orders typically include provisions detailing what the receiving party must do in an instance of a data breach, including how quickly the receiving party must notify the producing party of the breach.[72] Most importantly, the order generally includes provisions requiring the destruction or return of confidential information.[73]

While there is no federal rule mandating the inclusion of these provisions, the practice of including these provisions in protective or confidentiality orders has become an industry custom.[74] The practice is based on an underlying understanding among litigants that there is an assumption of confidentiality covering the data that is produced.[75] If a receiving party truly understood the transfer of information in discovery to confer an ownership interest in the information received, the receiving party would not agree to incur the burden of reasonably protecting that data. Even absent a formal rule, such provisions are so commonplace in protective and confidentiality orders that there is arguably an implied agreement to return or destroy the data after litigation.[76]

The producing party cannot be said to lose its ownership interest in the ESI that is produced when transferring data to comply with discovery obligations. But let's assume that the opposite is true, and that an ownership interest *is* transferred when data is produced in discovery. The receiving party now has a property interest over the ESI it has received. Would it now be permissible for the receiving party to add all the email addresses obtained from an opponent during discovery to a marketing database? If the receiving

---

71 *Id.* at 46.

72 *Id.* at 54.

73 *See id.* at 54-55 (stating that after the end of litigation, each party "must either return all Confidential . . . Information to the Disclosing Party or destroy such material, including all [forms] in which the Confidential Information may have been reproduced").

74 *See* Marcus, *supra* note at 43, at 9 ("These stipulated orders, which usually provide 'umbrella' protection for all materials designated confidential by the party producing them, have become the norm in many areas of federal practice.").

75 *See id.* at 11 ("The assumption of confidentiality carries over into the conduct of the discovery process. Far from being open to the public, discovery actually occurs in private.").

76 *Id.* at 10-11.

party truly has a property right in the ESI, and there is no implied agreement of nondisclosure in discovery, the receiving party could rightfully sell the list of email addresses to the highest bidder.

It is not just electronic documentary evidence that is transferred in discovery. Physical evidence is also transferred. Thus, the receiving party would not only gain a property right in the ESI; the receiving party would now become a partial owner of the physical evidence it receives. It does not require an in-depth analysis to explain why this is a ludicrous result. And yet the hypothetical could create even more problematic scenarios.

Consider the effect that the transfer of ownership interests would have on intellectual property rights. Could a receiving party now sue a party that has published a copyrighted work that had been produced in litigation? Copyright law has a particularly low threshold: only a "modicum of creativity" and originality is required to receive copyright protection.[77] Under the low threshold of copyright, almost all written works are copyrightable. If intellectual property rights also transfer with discovery, ownership of the copyright protections would extend to the receiving party. Along with the producing party, the receiving party would now share the right to reproduce, adapt, and distribute the copyrighted material.[78] A receiving party could now rightfully sue anyone who infringes on this copyright.

The illogical results of this hypothetical illustrate why a property right cannot possibly be transferred during the production of information and evidence in discovery. As a matter of common sense, no one believes that when things of major value are transferred in litigation (drug formulas, trade secrets, patents, or artistic works), the intellectual property rights are transferred to the receiving party. Logic dictates that it is true not only of high-value documents, but of all documents.

The producing party *must* maintain a property right over the transferred ESI. If a producing party merely transfers a temporary possessory interest over its property to a receiving party for the course of litigation, and the receiving party truly gains no ownership interest in the property, then the discovery process is primed for a bailment analysis.

In theory, a bailment is created every time there is a separation of ownership and possession of a good.[79] A bailment may be created by explicit agreement, finding, or implication.[80] The true owner of the property is known

77 Feist Publn's, Inc. v. Rural Tel. Serv. Co., Inc., 499 U.S. 340, 346 (1991).

78 *See* 17 U.S.C. § 106 (2012) (summarizing the exclusive rights held by copyright owners).

79 R. H. Helmholz, *Bailment Theories and the Liability of Bailees: The Elusive Uniform Standard of Reasonable Care*, 41 U. KAN. L. REV. 97, 97 (1992).

80 *Id.* at 98.

as the "bailor."[81] The possessory holder of the property is known as the "bailee."[82] A bailment exists when there is 1) delivery, 2) acceptance, and 3) consideration of property.[83] Depending on the circumstances of the transfer of property, the bailee owes a certain level of care to protect the property of the bailee.[84] In discovery, the receiving party is the bailee and the producing party is the bailor. If the elements for a bailment are met in discovery, as I will analyze in Part IV, the bailee is under a legal obligation to care for the property of the bailor.

Three standards guide the world of bailment: extraordinary care, ordinary care, or gross negligence.[85] A breach of bailment action may either be founded in tort law or contract law where an explicit agreement to create a bailment exists.[86] A bailment action brought under tort law holds a bailee liable for losses resulting from the bailee's failure to exercise the appropriate standard of care.[87] These standards of care and when they apply will be explored in more detail in Part V. But first, this Comment will discuss the historical roadblocks that bailment theories have faced when introduced in past data breach litigation.

III. DATA SECURITY LITIGATION AND BAILMENT

Several courts have addressed the theory of bailment in the context of data breach litigation but have declined to extend bailment liability to electronic data that is lost or stolen. No court to date has fully developed the analysis.[88] No court has ever addressed the theory of bailment directly in the context of discovery obligations.

---

81 *See generally* Mark S. Dennis, *Bailee's Liability for Damage, Loss, or Theft of Bailed Property*, 46 AM. JUR. PROOF OF FACTS 3d 361 § 2 (2018).

82 *See generally id.*

83 *See* Charles E. Cullen, *The Definition of Bailment*, 11 ST. LOUIS L. REV. 257, 259-62 (1926) (discussing components that are commonly present in bailment transactions).

84 *See* JESSE DUKEMINIER, JAMES E. KRIER, GREGORY S. ALEXANDER, MICHAEL H. SCHILL & LIOR JACOB STRAHILEVITZ, PROPERTY 127 n.2 (8th ed. 2014) (explaining that the question of what obligations a bailee owes varies, where "some bailees were held to a standard of great care, some (such as finders) to a standard of minimal care, and the balance to an ordinary negligence standard of reasonable care under the circumstances. The modern view is that the latter standard should apply across the board"); Helmholz, *supra* note 79, at 99, 102 (noting that "the accepted view holds that a uniform standard of ordinary care prevails" but that "[b]ailees are frequently held to a higher standard of care").

85 *See* Dennis, *supra* note 81, § 19.

86 Rachel M. Kane, *Proof of Breach of Bailment in Cases Where Object of Bailment is in Form of Electronic Data*, 156 AM. JUR. PROOF OF FACTS 3d 1 § 2 (2016) ("An action for breach of bailment may sound in either tort or contract, at the plaintiff's option.").

87 *See* DW Data, Inc. v. C. Coakley Relocation Sys., Inc., 951 F. Supp. 2d 1037, 1049 (N.D. Ill. 2013) (applying Illinois state law, and finding that "[b]ailees will be liable for losses that result from their . . . failure to exercise [ordinary care]").

88 *See* Todd Ommen, *Bailment Claims: A Cause of Action in Data Breach Cases*, WEITZ & LUXENBERG (Apr. 14, 2015), https://www.weitzlux.com/blog/2015/04/14/bailment-claims-cause-

The consensus of courts in data security litigation has been that electronic data that is transferred does not constitute the "delivery" of property required for the creation of a bailment. The bailment theory to data breach was first addressed in *Richardson v. DSW, Inc.*[89] In *Richardson*, a class of consumer plaintiffs sued DSW under a bailment theory after a data security breach lead to the dissemination of stolen credit and debit card information.[90] The court rejected the plaintiffs' bailment theory.[91]

The Northern District of Illinois defined a bailment as "the delivery of property for some purpose upon a contract, express or implied, that after the purpose has been fulfilled, the property shall be redelivered to the bailor."[92] The *Richardson* court noted that intangible property, such as electronic data, may be the subject of a bailment in certain circumstances, but a successful bailment claim must include the delivery and return of the property.[93] Ultimately, because there was no agreement that DSW would return her credit card information to her, the plaintiff's bailment theory could not succeed.[94]

The bailment theory to data security litigation first introduced in *Richardson* later resurfaced in *Sony Gaming Networks* and *Target*. *Sony Gaming Networks* involved a nationwide class action brought against Sony following a massive data breach.[95] Hackers accessed Sony's network and stole the personal information of millions of Sony customers, including customers' "names, mailing addresses, email addresses, birth dates, credit and debit card information," and more.[96]

The class alleged a variety of claims, including a claim for breach under a theory of bailment.[97] The *Sony* court quickly dismissed the bailment claim, reasoning that the plaintiff's electronic personal information could not be "construed to be personal property so that the [p]laintiffs somehow 'delivered' this property to Sony and then expected it to be returned."[98]

The issue was addressed again in *Target* following a massive data breach of Target's retail stores.[99] Hackers successfully breached Target's data security

action-data-breach-cases/ [https://perma.cc/5F7T-UUXD] ("Bailment is a long-standing, well-developed, and relevant cause of action that deserves better analysis and evaluation in data breach cases than it has received from courts to date.").

89 No. 05-4599, 2005 WL 2978755 (N.D. Ill. Nov. 3, 2005).

90 *Id.* at *1.

91 *Id.* at *4.

92 *Id.*

93 *Id.*

94 *Id.*

95 *In re* Sony Gaming Networks & Customer Data Sec. Breach Litig., 903 F. Supp. 2d 942, 974 (S.D. Cal. 2012).

96 *Id.* at 950.

97 *Id.* at 974.

98 *Id.*

99 *In re* Target Corp. Customer Data Sec. Breach Litig., 66 F. Supp. 3d 1154, 1157 (D. Minn. 2014).

systems and stole the personal information and credit and debit card information of approximately 110 million customers of Target.[100] Once again, the class of plaintiffs alleged a bailment theory for injuries suffered from Target's failure to adequately protect their electronic information.[101]

Citing both *Richardson* and *Sony Gaming Networks*, the *Target* court rejected the plaintiff's bailment claims, reasoning that the electronic data that was stolen could not be returned to the bailor.[102] However, the *Target* Court "provided essentially no analysis of bailment claims, the standard of care applicable, or the issue of whether 'return' of the property is an element at all, let alone where the property is intangible."[103]

The consideration of bailment liability in cases of data breach has been underdeveloped and overlooked. The courts here engaged in the wrong analysis of the issue of "return." The analysis should not focus on whether the property be physically returned, but should instead focus on the temporary nature of the baliee's possessory interest. Companies like Target and Sony are not permitted to retain customer credit card and personal information indefinitely. The companies receive a digital copy of the information, but they certainly do not obtain an ownership interest over an individual's credit card or personal data. In some cases, these companies are required by law to destroy the credit card and personal data after a certain period.[104] Moreover, by destroying the data, they return to the customer the right (or fact) that they are the sole possessor of the personal data and information in question.

Customers and these companies have an implied agreement to destroy the data copies following the purchase transaction. Industry standards and legislation often expressly prohibit the retaining of certain credit card and customer data. In *Target*, for example, the consumer plaintiffs cited Minnesota law preventing companies from retaining credit card security code data or PIN verification data from more than forty-eight hours after the transaction has been authorized.[105] A company that fails to delete the data within forty-eight hours of authorization is in violation of the statutory time limitation.[106]

The credit card industry itself has established guidelines requiring the deletion of certain data. The Payment Card Industry Data Security Standards

---

100 *Id.*

101 *Id.* at 1177.

102 *See id.* ("Even if Plaintiffs are correct that intangible property such as their personal financial information can constitute property subject to bailment principles, they have not—and cannot—allege that they and Target agreed that Target would return the property to them.").

103 Ommen, *supra* note 88.

104 *See, e.g.*, MINN. STAT. ANN. § 325E.64 (West 2007) (providing for liability for an entity engaged in business in Minnesota that retains security code data, a PIN verification code number, or the contents of magnetic stripe data collected in connection with a transaction).

105 *Target*, 66 F. Supp. 3d at 1168.

106 MINN. STAT. ANN. § 325E.64 (West 2007).

direct companies to retain consumer data no longer than necessary for business, legal, or regulatory purposes and to regularly purge unnecessarily stored data.[107] The Standards also direct companies to purge consumer authentication data after the transaction is authorized.[108] Ultimately, companies like Sony and Target are under an obligation to destroy customers' sensitive data after the authorization of the transaction.

A look into the plaintiffs' complaint and brief in *Target* is instructive. The plaintiffs alleged in their complaint that "Target failed to return, purge or delete the personal and financial information of Plaintiffs and members of the Class at the conclusion of the bailment (or deposit) and within the time limits allowed by law."[109] The plaintiffs further alleged that there was an implied agreement for Target to comply with industry and legal standards.[110] As a result of the breach, plaintiffs alleged their financial and personal information was "damaged and its value diminished."[111]

The courts in these data breach litigations failed to recognize that when there is an obligation on the company to delete the data, there is a viable argument for bailment liability. The issue is not merely whether the data was returned, but whether the data was dealt with according to the directions of the bailor.[112] Despite the courts' holdings in these consumer breach cases, the plaintiffs' bailment theories did not depend on the literal return of the data.

While the consumers gave no explicit instructions to the companies receiving their data, there was a legal obligation on the company to delete the data and a credible implicit expectation that the company adequately safeguard customers' data and comply with the law. The companies did not deal with the consumers' intangible property according to their implied and legal obligations, arguably satisfying the bailment requirement that the data was never returned, or was returned in a damaged form. The personal data of the consumers was irreparably damaged by the data breach. As a result, the claims as pleaded by the consumer plaintiffs in *Sony Gaming Networks*, *Target*, and *Richardson*, gave rise to a plausible theory of bailment liability.

---

107 PAYMENT CARD INDUSTRY SECURITY STANDARDS, COUNCIL, PAYMENT CARD INDUSTRY DATA SECURITY STANDARDS 14 (2010).

108 *See id.* (noting that companies should not "store sensitive authentication data after authorization").

109 Consumer Plaintiffs' First Amended Consolidated Class Action Complaint at 118, *In re* Target, 2014 WL 7014791 (No. 14-2522).

110 Consumer Plaintiffs' Memorandum in Opposition to Defendant's Motion to Dismiss at 58-60, *In re* Target, 2014 WL 7014791 (No. 14-2522).

111 Consumer Plaintiffs' First Amended Consolidated Class Action Complaint at 118, *In re* Target, 2014 WL 7014791 (No. 14-2522).

112 *See supra* note 26 and accompanying text; *see also* Home Indem. Co. v. Harleysville Mut. Ins. Co., 166 S.E.2d 819, 824 (S.C. 1969) (noting that after the terms of the bailment contract have been fulfilled, the chattel "shall be redelivered to the bailor, or otherwise dealt with according to his directions").

Regardless of whether the courts engaged in the correct bailment analysis, the rejection of the bailment theories in the data breach context does not preclude the exploration of bailment principles in the discovery process. The context of discovery differs from traditional data breach litigation in ways that make the application of bailment theory more feasible. First, as made clear in *Seattle Times*, the receiving party's rights to the data are limited and only for a limited purpose. Second, the production of the data is not voluntary and compels the production of information that the requesting party would not be entitled to otherwise. Third, the general presumption is that the receiving party will not keep the information that is produced. Part V will explore why the transfer of electronic data in discovery meets all the elements required for the application of bailment liability.

IV. THE MODERN DEFINITION OF BAILMENT INCLUDES ESI

Before applying the legal standards of bailment to the discovery context, I must establish that electronic information transferred through the discovery process is property that may be subject to bailment liability.

A bailment only applies to certain types of property.[113] Historically, bailment law only applied to tangible property such as chattels.[114] Whether bailment applies to intangible property, such as electronic data, has long been a matter of substantial debate.[115] For example, the Northern District of California previously concluded that social security numbers and credit card information are not bailable property.[116]

It is well established that "information" may be the subject of a bailment.[117] For example, a court has found information contained in a letter is property subject to be bailed.[118] Similarly, scholars have argued that information contained in an email is property under bailment theory.[119] Therefore, information in itself may be bailable property.

---

113 *See* 8A AM. JUR. 2D *Bailments* § 3 (2018) (overviewing the types of property that may be subject to bailment).

114 *See, e.g.*, Samuel Stoljar, *The Early History of Bailment*, 1 AM. J. LEGAL HIST. 5, 31-32 (1957) (discussing a late eighteenth-century bailment case that involved tangible property).

115 *See, e.g.*, Thyroff v. Nationwide Mut. Ins. Co., 864 N.E.2d 1272, 1275-77 (Mass. App. Ct. 2007) (analyzing whether traditional torts should apply to intangible data).

116 *See* Ruiz v. Gap, Inc., 540 F. Supp. 2d 1121, 1127 (N.D. Cal. 2008) (applying California law to find that a social security number could not be personal property under bailment theory), *aff'd*, 380 F. App'x. 689 (9th Cir. 2010).

117 *See* 8A AM. JUR. 2D *Bailments* § 3 n.1 (2018).

118 Liddle v. Salem Sch. Dist., 619 N.E.2d 530, 531 (Ill. App. Ct. 1993).

119 *See, e.g.*, Jonathan J. Darrow & Gerald R. Ferrera, *Who Owns a Decedent's E-Mails: Inheritable Probate Assets or Property of the Network?*, 10 N.Y.U. J. LEGIS. & PUB. POL'Y 281, 306 (2007) (noting that "[e]ven the intangible information contained in an email may be bailed"). *But see* Rachel M. Kane, *Proof of Breach of Bailment in Cases Where Object of Bailment Is in Form of Electronic Data*, 156

Courts have repeatedly held that electronic data may be intangible property subject to a bailment. Courts have interpreted bailments of electronic data to include computerized data stored on a hard drive,[120] information stored electronically on a computer,[121] computer programs,[122] and financial data stored on a computer.[123]

Notably, the information transferred in discovery is not the original data, but rather is a copy of the data. Therefore, the ESI is simultaneously in the possession of both the producing and the receiving party. This runs afoul of traditional bailment principles requiring that the bailor take exclusive possession of the property.[124] The exclusivity requirement is designed to prevent the creation of bailments where the bailee maintains control over the property, particularly in cases of shared possession.[125]

The exclusivity requirement, however, should not be applied to bailments of intangible property. Intangible property is easily copied and disseminated, and thus is almost never in the exclusive possession of the bailee. Although both the producing and receiving party possess the information, the transfer of ESI in discovery cannot be conceptualized as a shared possession. By producing a copy of ESI to a receiving party, the producing party is relinquishing control over that data. They are placing that ESI in the care of the receiving party to be stored at greater risk of data security threats.[126] This temporary "storage" transaction is not the type of bailment that the exclusivity requirement seeks to prevent but rather is precisely the type of property exchange that gives rise to a bailment.[127] Furthermore, recent case law has suggested that the exclusivity requirement should no longer be applied to electronic data.[128]

Even if the ESI transferred in discovery is at odds with the bailment exclusivity requirement, an electronic copy of the data may be easily

---

AM. JUR. PROOF OF FACTS 3d 1 § 11 (2016) (illustrating circumstances where a bailment obligation is not breached by a recipient of electronically conveyed images if the recipient complies with the sender's instructions for deletion, notwithstanding the subsequent dissemination of the data).

120 Bridge Tower Dental, P.A. v. Meridian Comput. Ctr., Inc., 272 P.3d 541, 546 (Idaho 2012).

121 Shmueli v. Corcoran Grp., 802 N.Y.S.2d 871, 877-78 (Sup. Ct. 2005).

122 David Barr Realtors, Inc. v. Sadei, No. 03-97-00138, 1998 WL 333954, at *3 (Tex. App. June 25, 1998).

123 *See id.* at *3, 8.

124 *See, e.g.*, Beech Transp. v. Critical Care Servs., No. 01-0292, 2001 Minn. App. Lexis 1129, at *9 (Minn. Ct. App. Oct. 9, 2001) (concluding that there was no bailment where the bailor did not have exclusive possession, control, and dominion over the property).

125 *See also* Herrington v. Verrilli, 151 F. Supp. 2d 449, 459 (S.D.N.Y. 2001) (differentiating "non-bailment 'park and lock'" situations from bailment).

126 *See supra* notes 3–4 and accompanying text.

127 *See* 8A AM. JUR. 2D *Bailments* § 5 n.7 (2018) (citing example of the storage of goods in a warehouse).

128 *See supra* notes 120–123 and accompanying text.

construed as entirely new property. Under this conception, the copy of the ESI is in the sole possession of the receiving party for whom the copy was made, and thus the exclusivity requirement would be satisfied.

In either case, the definition of intangible personal property for bailment purposes must include copies of electronic data. Intangible, electronically stored information that is copied and transferred to the receiving party may be held in bailment if this transfer meets the required elements for the creation of a bailment.

V. APPLICATION OF BAILMENT ELEMENTS TO THE DISCOVERY PROCESS

A bailment only arises when certain essential elements are met.[129] The transfer of information through the discovery process satisfies the prerequisite elements for the creation of a bailment. As previously mentioned, a bailment exists when there is 1) delivery, 2) acceptance, and 3) consideration of property.[130] First, a bailment must involve the delivery of possession or control over property from the bailor to the bailee, as well as the return of the property in an undamaged condition.[131] Second, there must be an agreement by the bailee, either explicit or implied, to accept possession or control over the property.[132] Third, a bailment may only exist when there is an exchange of something of value.[133] Electronic data in discovery may be evaluated under bailment theory as it is produced and delivered to a receiving party who accepts the data and receives the benefit of information relevant to their claims and defenses in litigation.

The consideration element is satisfied and may be disposed of without discussion. For consideration to be satisfied, there must be a transfer of something of value. The purpose of discovery is to obtain the information necessary for a party to prove their claims and defenses. Information that is relevant to a party's claims and defenses has innate value in litigation. As a result, the "consideration" element is satisfied. My analysis will focus on the delivery and acceptance elements.

---

129 *See supra* note 25.

130 *See also* William King Laidlaw, *Principles of Bailment*, 16 CORNELL L. REV. 286, 289-91 (1931) (applying bailment requirements to a particular set of facts).

131 *See supra* note 25 § 1 ("Inherent in the bailment relationship is the requirement that the property be returned to the bailer, or duly accounted for by the bailee, when the purpose of the bailment is accomplished.").

132 *See id.* ("A bailment is created . . . pursuant to an express or implied contract to fulfill that trust.").

133 *See id.* ("A bailment relationship can be implied by law whenever the personal property of one person is acquired by another . . . .").

A. *Delivery and Return of the ESI*

The production and transfer of electronic data in discovery constitutes a delivery of goods and creates a duty in the bailee to return the goods when the bailment ends. Some scholars argue that the transmission of electronic information does not constitute a delivery, and thus can never be a bailment.[134] This was the ultimate failing of the bailment theories in the data security litigation covered in Part IV. The shortcomings that existed in *Richardson*, *Target*, and *Sony Gaming Networks*, however, do not apply to the discovery process.

There must be a change in possession of the property to impute a bailment. The "delivery" and "return" of intangible property is precisely what happens in discovery. Parties in litigation issue requests for production to obtain information in the possession of their opponent in hopes of using that information to meet the elements of their claim or defense.[135] Recall that in Part II, I established that a receiving party gains no ownership interest in the information obtained from their adversary.[136] Just as in a bailment, the receiving party obtains possession of the relevant information from the producing party, but does not gain an ownership interest in the information. A temporary possessory interest is created. At no point does the producing party lose title to the information that is transferred. The receiving party is merely "warehousing" the ESI for use during litigation.[137] The production of ESI is equivalent to the delivery of bailed property.

A bailee "is under a strict duty to return the bailed goods at the expiration of the term of bailment."[138] If bailed property is not returned to the bailor, it must at least be disposed of according to the bailor's directions.[139] In discovery, must a receiving party return the electronic data to the producing party at the end of discovery? *Seattle Times* dealt with this issue: Could the

---

134 *See* Lim, *supra* note 17, at 94-95 ("[D]ata security does not actually involve the delivery of property or information. . . . [W]hen data is secured electronically . . . there is no change in possession and so it is hard to see how simply securing information could constitute a bailment.").

135 *See* FED. R. CIV. P. 34(a)(1)(A) ("A party may serve on another party a request . . . to produce . . . any designated documents or electronically stored information . . . .").

136 *See supra* Part II.

137 Warehousing refers to the business of paying for the storage of goods. HOWARD J. ALPERIN, 14 MASS. PRAC., SUMMARY OF BASIC LAW § 2:15 (5th ed. 2017); *see, e.g.*, Carr v. Hoosier Photo Supplies, Inc., 441 N.E.2d 450, 452-53 (Ind. 1982) (discussing rolls of photographic film lost by a film developer); Mieske v. Bartell Drug Co., 593 P.2d 1308, 1313 (Wash. 1979) (discussing destruction of reels of movie film). Warehousing provides a clear example of an explicit agreement, usually under contract, to enter a bailment to store goods temporarily and for the warehouse to protect those goods from harm.

138 Walton Commercial Enters., Inc. v. Ass'ns, Conventions, Tradeshows, Inc., 593 N.E.2d 64, 67 (Ohio Ct. App. 1990).

139 *See* Home Indem. Co. v. Harleysville Mut. Ins. Co., 252 S.C. 452, 460 (1969) ("[A]fter the purpose [of the bailment] has been fulfilled, then the chattel shall be redelivered to the bailor, or otherwise dealt with according to his directions.").

newspaper have published the information it received during discovery, or was it under some obligation to "return" or destroy the data it received?

The answer turns on whether information transferred in discovery is truly private such that it must be returned to the producing party. Private information that is publicly disclosed cannot be said to be "returned" for the purposes of a bailment. The *Seattle Times* Court noted that some discovery information may be publicized. Information that would traditionally be public may be disseminated.[140] Purely private information transferred in discovery, however, may not be disseminated; said differently, "[a] litigant has no First Amendment right of access to information made available only for purposes of trying his suit."[141]

The Supreme Court has held that discovery in civil litigation is not part of the open civil process, but rather is a private affair.[142] Some scholars have argued that although the "Supreme Court has unequivocally declared that privacy interests are protected by Rule 26(c) . . . that does not mean that this protection applies in all commercial cases."[143] This suggests that there is no blanket rule protecting the confidentiality of information transferred in discovery without a protective or confidentiality order in place. This assertion, however, ignores the temporary nature of the discovery process. The process of obtaining discovery ends at a time set by the court, but the true end of discovery is the termination of the litigation.

Litigation never goes on forever. After a lawsuit, all confidential information disclosed during discovery generally must be returned to the producing party.[144] The receiving party's limited right to use and keep the information has ended. Some critics of protective orders have argued that all information disclosed in discovery should be public.[145] While there are some circumstances in which information may not be returned to the producing party, the baseline presumption is that at the end of litigation the receiving party must either return the ESI or destroy it according to the producing

---

140 *Cf.* Seattle Times Co. v. Rhinehart, 467 U.S. 20, 33 (1984) ("[P]retrial depositions and interrogatories are not public components of a civil trial. . . . [R]estraints placed on discovered, but not yet admitted, information are not a restriction on a traditionally public source of information.").

141 *Id.* at 32.

142 *See In re* Reporters Comm. for Freedom of the Press, 773 F.2d 1325, 1337 (D.C. Cir. 1985) (Scalia, J.) ("Traditionally, absent a statute or court order, even parties to the case did not have the right to inspect depositions taken at the behest of their opponents.").

143 Richard L. Marcus, *The Discovery Confidentiality Controversy*, 1991 U. ILL. L. REV. 457, 492 (1991).

144 This understanding is supported by provisions in the model federal protective order provided by the Sedona Conference, see THE SEDONA CONFERENCE, *supra* note 8, at 54-55 ("Upon final resolution of this Litigation the Parties will certify that all Confidential Material and/or Highly Confidential Material has been returned to the Producing Party and/or been destroyed in a secure manner.").

145 For a full analysis of the arguments of these critics, see Marcus, *supra* note 143, at 459-66.

party's instructions.[146] When the information involved is confidential, the return or destruction of the ESI is a certainty because a protective or confidentiality order will nearly always be issued.[147] It is arguably malpractice for an attorney to not ensure that the confidential information of their client was thoroughly protected. But even absent a discovery order, a receiving party gains no ownership interest in the ESI received.[148] Because the information remains private at the termination of litigation and must be dealt with according to the producing parties' instructions, the data that was transferred is effectively "returned" to the producing party.

B. *Agreement and Acceptance of the ESI*

The receiving party may be presumed to have accepted the electronic information. It is unlikely that any party ever declines to receive the information sent by the producing party in discovery because they hope that the information obtained will help them prove their claims or defenses. In fact, much of the information transferred in discovery would be specifically requested by the receiving party.

In federal court, parties are obligated to disclose certain information through initial disclosures.[149] The remaining data produced is either sent willingly in response to requests for production,[150] or unwillingly pursuant to a court order or subpoena.[151]

Although a party actually accepts the information transferred in discovery, is there an explicit or implied agreement to accept the information? The transfer of ESI in discovery can be construed as either an explicit or an implied agreement. A request for production may be understood as an explicit agreement to accept the information because the ESI that is transferred has been requested by the receiving party.

Even absent a direct request for production, the transfer of ESI in discovery may constitute an implied agreement. It is well settled that "[a] bailment relationship can be implied by law whenever the personal property of one person is acquired by another and held under circumstances in which principles of justice require the recipient to keep the property safely and

---

146 *Supra* note 144.

147 *See* Marcus, *supra* note 43, at 10-11 (summarizing procedures for ensuring the privacy of confidential information during and after the conclusion of litigation).

148 *See supra* Part II.

149 *See* FED. R. CIV. P. 26(a)(1) (listing numerous documents and pieces of information that "a party must, without awaiting a discovery request, provide to the other parties").

150 *See generally* FED. R. CIV. P. 34 (describing what information and documentation parties can request from each other and procedures for doing so).

151 *See generally* FED. R. CIV. P. 37 (detailing when a party may seek court-ordered compulsion of production of discoverable materials).

return it to the owner."[152] This is precisely what happens in discovery. The discovery process involves the transfer of intangible property, or ESI, belonging to the producing party to the receiving party. The receiving party then proceeds to hold this ESI over the course of litigation and ultimately returns the ESI to the possession of the producing party after the conclusion of the litigation.

This Comment seeks to establish that ESI obtained in discovery is "held under circumstances in which principles of justice require the recipient to keep the property safely."[153] In the context of ESI, keeping the property safe means establishing adequate safety measures to protect the data from data security threats and hacking. This baseline obligation to keep the property safe does not currently exist. Protective and confidentiality orders fill this gap in the law. They serve as explicit agreements to ensure that ESI is kept safe.

But even in the absence of a protective order, there is an existing implied agreement to keep the property of the producing party safe. This can be better understood by a comparative analysis considering the obligations that are placed on a producing party in discovery. Producing parties are responsible for preserving relevant electronically stored information for discovery.[154] A producing party that fails to take reasonable steps to preserve relevant data to a reasonably anticipated litigation may be subject to sanctions.[155] In other words, a producing party that loses data that is in its possession, custody, and control can be subject to fines, cost shifting, special jury instructions, and, in extreme cases, case-altering sanctions such as an adverse inference.[156] When it comes to protecting and preserving ESI, producing parties are held to a high standard.

However, there is no precedent for issuing sanctions against a receiving party who fails to adequately protect the property of the producing party when a protective order is not in place, even though companies invest massive amounts of money in their information technology infrastructure to protect

---

152 8A AM. JUR. 2D *Bailments* § 1 (2018).

153 *Id.*

154 *See, e.g.*, Zubulake v. UBS Warburg LLC, 220 F.R.D. 212, 218 (S.D.N.Y. 2003) ("A party or anticipated party must retain all relevant documents . . . in existence at the time the duty to preserve attaches, and any relevant documents created thereafter . . . . [T]here are many ways to manage electronic data, [so] litigants are free to choose how this task is accomplished.").

155 FED. R. CIV. P. 37(e); *see, e.g.*, Silvestri v. Gen. Motors Corp., 271 F.3d 583, 590 (4th Cir. 2001) (noting that courts have "[t]he right to impose sanctions" for failing to preserve relevant evidence, an ability that "arises from a court's inherent power to control the judicial process and litigation").

156 *See* FED. R. CIV. P. 37(e)(2)(B) (providing that, where ESI that should have been stored is lost due to a party's failure to take precautionary measures and intent to deprive their opponent of the information, the court may issue an adverse inference jury instruction).

their own proprietary data.[157] With such stringent obligations placed on the producing party to protect the ESI, it is highly implausible that the receiving party has no obligation whatsoever to protect the data that they receive.

Consider the following scenario. A large multinational corporation is sued in a products liability class action litigation. Suppose the product is a highly advanced artificial knee replacement that has recently caused medical complications. As soon as the corporation becomes aware of these complications, it "reasonably anticipates" litigation and a preservation obligation is triggered.[158] The class then issues lengthy discovery requests seeking massive amounts of proprietary, trade secret, and confidential information.

Suppose, for purposes of this hypothetical, that no protective or confidentiality order is executed. The corporation produces millions of pages of electronic data in response to the plaintiffs' discovery requests. Included in their production is the highly sensitive schematic of their knee replacement device. Soon after, the plaintiff's law firm is hacked and hackers upload the highly sensitive schematic to the internet. What recourse does the corporation have? The corporation may seek recourse outside of the present litigation by opting to sue for negligence and failure to take reasonable security precautions. However, discovery law itself offers the party no immediate recourse.

Now suppose an alternate scenario where the plaintiffs request all communications relating to the knee replacement device between the time that the corporation reasonably anticipated litigation to the present. During this time, the corporation was obligated to take reasonable steps to prevent the loss of relevant data. But, due to the corporation's failure to institute an effective and reasonable litigation hold, large chunks of relevant communications were permanently and irreplaceably deleted as a part of the corporation's IT function that automatically deleted emails after two weeks.[159] Because the corporation failed to take reasonable steps to preserve the data, the corporation would be subject to sanctions and other penalties.

In both scenarios, data was lost or placed at substantial risk. Yet only the corporation faces repercussions under discovery law, while the class of plaintiffs escapes unscathed. The corporation must turn to tort law for a remedy, and may only do so after the data has been irreparably damaged or lost. This imbalance has no place in a judicial system that is guided by reason. There must be some recourse to protect the producing party under discovery law.

---

157 *See, e.g.*, Kate Fazzini, *Facebook: We're Investing in Security and it Will Hurt Profits*, WALL ST. J. (Dec. 11, 2017, 5:03 PM) (detailing Facebook's plans to double its cybersecurity staff and expand security engineering efforts, even though doing so would take resources away from profit-generating projects).

158 *See Zubulake*, 220 F.R.D. at 217 ("[A]nyone who [reasonably] anticipates being a party . . . is under a duty to preserve what it knows, or reasonably should know, is relevant in the action [and/or] is reasonably calculated to lead to the discovery of admissible evidence . . . .").

159 This is highly unlikely, but let's assume this for the purposes of the hypothetical.

If there is no recourse under the law, or no agreement that the receiving party will keep the data safe, it would be negligent of the producing party and its counsel to produce the data in the first place. Without a protective order, a party would be handing sensitive data to a third party without any assurance that they will protect the data using proper data security measures. Thus, without a common-law obligation or recourse in the event of a data breach, it would be negligent for counsel for the producing party to turn over ESI in discovery in terms of data security.[160] This cannot be the answer.

It can be stated with a reasonable degree of certainty that a receiving party has at least *some* obligation arising out of an explicit or implied agreement to protect the data of the opposing party.[161]

C. *Data Breach and "Damaged" ESI*

The production of electronic data in discovery is primed for the application of a bailment analysis. Since it has been established that the transfer of data in discovery satisfies the elements of a bailment, we must determine whether lost or stolen data held by the receiving party would permit a claim of bailment liability. Recall that if a bailment exists, four elements must be satisfied to bring a successful bailment claim for electronic data: "1) the existence of an agreement, express or implied, to create a bailment; 2) delivery of the electronic data; 3) acceptance of the electronic data by the bailee; and 4) nonreturn or redelivery of the electronic data in a damaged condition."[162]

The first three elements have been established. Thus, a producing party may bring a successful claim for bailment liability only if it can demonstrate the "nonreturn or redelivery of the electronic data in a damaged condition."[163] But, may data that is breached through hacking, cyber-attacks, or corporate espionage be considered "damaged?"

---

160 Knowingly placing your client's electronic data at risk may be both malpractice and a violation of the Model Rules of Professional Responsibility. Lawyers have a duty to protect client information from data breaches. *See* AM. BAR. ASS'N, FORMAL OPINION 483: LAWYERS' OBLIGATIONS AFTER AN ELECTRONIC DATA BREACH OR CYBERATTACK 7 (2018) (explaining that lawyers have an obligation under Model Rule 1.6(c) to take reasonable efforts to prevent the inadvertent disclosure or unauthorized access of client's information, and that "[t]hese reasonable efforts could include (i) restoring the technology systems as practical, (ii) the implementation of new technology or new systems, or (iii) the use of no technology at all if the task does not require it, depending on the circumstances").

161 *See, e.g.*, THE SEDONA CONFERENCE, THE SEDONA PRINCIPLES (THIRD EDITION): BEST PRACTICES RECOMMENDATIONS & PRINCIPLES FOR ADDRESSING ELECTRONIC DOCUMENT PRODUCTION 178-79 (2018) ("Just as responding parties are obligated to take reasonable steps that are proportional to the needs of the case to find and produce requested information within the scope of discovery under Rule 26(b)(1), a requesting party should take reasonable steps to secure the information they requested and received.").

162 Kane, *supra* note 86.

163 *Id.*

Bridge Tower Dental, P.A., v. Meridian Computer Center, Inc.[164] provides an example of the damaged condition requirement for bailment liability. The defendant in *Bridge Tower*, a computer service company, owed a duty of reasonable care to protect two hard drives delivered by the plaintiff under a bailment theory.[165] The defendant accidentally deleted the data from one of the hard drives and returned the data in a "damaged state."[166] When property is delivered in a damaged state or not delivered at all to the bailor, "the law presumes negligence to be the cause, and casts upon the bailee the burden of showing that the loss is due to other causes consistent with due care on his part."[167] The *Bridge Tower* court ruled in favor of the plaintiff under a bailment theory of liability.[168]

It is undeniable that the deletion of data from a hard drive constitutes damage of property. It is less clear, however, whether a data breach can be construed as damaging the electronically stored information. The district court in *In re Sony* dealt with claims that a data breach caused by hacking resulted in property damage to the Sony customers whose personal information was stolen.[169] The court dismissed the property damage tort claims because the plaintiffs failed to allege "what property was allegedly damaged, or how the alleged property damage was proximately caused by Sony's breach."[170]

For purposes of bailment liability, property is "damaged" when it is not returned in the same condition it was in when it was delivered.[171] Data that has been hacked has been fundamentally and irreparably changed, and thus is not returned in the same condition that it was in when it was delivered. The most evident change arises from the decrease in value that results from hacking. Consider the hacking of a trade secret. A trade secret is "information including a formula, pattern, compilation, program, device, method, technique or process, that derives independent economic value."[172] Most modern trade secrets are maintained in an electronic format. By definition, value is stored in the electronic data that makes up a trade secret. When that electronic data is breached and accessed by hackers, it suffers a loss of value that equates to a damaged condition of the data.[173]

---

164 272 P.3d 541 (Idaho 2012).

165 *Id.* at 546.

166 *Id.*

167 *Cluer v. Leahy*, 256 P. 760, 761 (Idaho 1927).

168 *Bridge Tower*, 272 P.3d at 542.

169 WILLISTON & LORD, *supra* note 26, at 950.

170 *In re* Sony Gaming Networks & Customer Data Sec. Breach Litig., 996 F. Supp. 2d 942, 964 (S.D. Cal. 2014), *order corrected* No. 11MD2258, 2014 WL 12603117 (S.D. Cal. Feb. 10, 2014).

171 Kane, *supra* note 86, at § 6.

172 59 A.L.R. 4th 641 § 3 (1988).

173 *See* Brian T. Yeh, *Protection of Trade Secrets: Overview of Current Law and Legislation*, CONG. RES. SERV. 2 (2016) ("U.S. companies annually suffer billions of dollars in losses due to the theft of

Recall the scenario posed in Section V.B hypothesizing an artificial knee replacement products liability litigation. In that hypothetical, hackers breached the plaintiff's law firm, obtained highly sensitive trade secret information surrounding the development of the corporation's product, and leaked the information on the Internet. The corporation might have spent tens of millions of dollars in research and development to create their product, only to see the schematic widely disseminated in a singular breach. This would result in a massive decrease in the informational value of the trade secret. When this information is returned at the end of litigation, it is returned in an undeniably damaged condition.[174] A data breach can cause significant damage to ESI.

The transfer of ESI in discovery satisfies the prerequisite elements for the creation of a bailment and the application of bailment liability. The property principle of bailment may therefore supply the framework to set a standard in the discovery context.

VI. THE NEW BASELINE STANDARD

Now that bailment's ability to supply the standard of care in discovery has been established, I return to the question: when there is no protective order in place, what duty is owed by the receiving party to protect the information of the producing party?

The duty of care a bailee must exercise over the property depends on the circumstances surrounding the bailment. When there is a contractual agreement to enter a bailment, the standard of care established in the contract controls.[175] In the absence of an agreement, bailments can arise in involuntary or implied circumstances.[176] Under the traditional conception of bailment liability, a bailment may fall into one of three categories: 1) for the benefit of both the bailor and bailee, 2) for the sole benefit of the bailor, or 3) for the

their trade secrets by employees, corporate competitors, and even foreign governments. Stealing trade secrets has increasingly involved the use of cyberspace, advanced computer technologies, and mobile communication devices, thus making the theft relatively anonymous and difficult to detect.").

174 Data breaches can also cause companies significant losses in profit. *See* Elizabeth A. Harris, *Data Breach Hurts Profit at Target*, N.Y. TIMES (Feb. 26, 2014), http://www.nytimes.com/2014/02/27/business/target-reports-on-fourth-quarter-earnings.html?_r=0 [https://perma.cc/S7Q8-YTXG] ("The widespread theft of Target customer data had a significant impact on the company's profit, which fell more than 40 percent in the fourth quarter.").

175 *See* Helmholz, *supra* note 79, at 110 (noting courts have "determined that 'it is [the bailee's] contract which must measure the extent of his liability,' and, if there has been damage, this contractual undertaking results in liability without fault").

176 *Id.* at 98.

sole benefit of the bailee.[177] Each classification traditionally carries its own duty of care standard.

A bailment that both benefits the bailor and bailee is mutually beneficial. Mutually beneficial bailments commonly arise in circumstances where the bailee is paid to protect the property of the bailor. For example, a hotel that stores valuables and bags for its patrons creates a mutually beneficial bailment. When the bailment is mutually beneficial, the bailee owes ordinary care to protect the property of the bailor.[178]

Bailments that only benefit the bailor are often involuntary. For example, when someone asks a stranger to "keep an eye on their bag," a bailment is created that is for the sole benefit of the bailor. When a bailment only benefits the bailor, the bailee can only be liable for gross negligence in failing to protect the property of the bailor.[179] In the foregoing example, the bag-monitoring stranger would only be liable for gross negligence in failing to keep the bag safe.

In contrast, an example of a bailment for the sole benefit of the bailee occurs when an individual lends their car to a friend and receives nothing in return. When a bailment only benefits the bailee, the bailee owes extraordinary care to protect the property of the bailor.[180] In this scenario, the friend owes extraordinary care to keep the car safe, as he is receiving the full benefit of the property's use.

So where does the transfer of ESI in the discovery process fit into the bailment standards of care? The transfer of information during discovery can only be construed as being mutually beneficial or for the sole benefit of the bailee. Therefore, depending on how the bailment is understood, the receiving party either owes ordinary care or extraordinary care to protect the ESI of the producing party.

The most logical construction of the discovery process is as a "mutually beneficial" bailment. The receiving party has the obvious benefit of obtaining information that may be used to prove their claims or defenses. The producing party receives a benefit from complying with their discovery obligations: producing relevant information protects the producing party from adverse court orders and potential sanctions.

---

177 *See* James L. Buchwalter & Karl Oakes, 8 C.J.S. *Bailments* § 14 (2018) (noting that an "implied-in-fact bailment depends on the surrounding facts"); *see also* John T. Handy Co. v. Carman, 648 A.2d 1115, 1122 (Md. Sp. App. 1994) (recognizing the validity of an implied bailment).

178 *See* Kurt Philip Autor, *Bailment Liability: Toward A Standard of Reasonable Care*, 61 S. CAL. L. REV. 2117, 2131 (1988) (describing the varying standards of care owed in a bailment as "either slight, ordinary, or great—and, accordingly, liability is imposed only for corresponding levels of negligence—gross, ordinary, or slight. Thus, a party held to a duty of slight care is liable for gross negligence; if the duty is one of ordinary care then liability will be imposed for only ordinary negligence; and if there is a duty of great care, the bailor is liable for mere slight negligence").

179 *Id.*

180 *Id.*

Another benefit arises from cooperating with the opposing party: the expectation of a reciprocal production of documents. Parties always fill the roles of both the producing and receiving party in discovery. While Party A may not receive a direct benefit from making a production of data to Party B, Party A will expect Party B to make a production in response to their own discovery requests. Arguably both parties receive the benefit of obtaining information from their opposing party in the broader discovery context. This suggests that this transaction is not for the *sole* benefit of the bailee, and thus the standard of extraordinary care does not apply to the discovery process. The transfer of information in discovery is mutually beneficial, and the guiding standard should be ordinary care.

What constitutes ordinary care in data security should be understood through two prongs: "(1) what security measures the requesting party must have in place to protect the data and (2) what the requesting party must do in response to a breach of its security."[181]

First, the ordinary care standard considers what security measures make up a system of reasonable data security. Depending on the context, there is a great deal of variation as to what security measures are included in protective orders. In cases of extreme sensitivity, a producing party may only allow the ESI to be reviewed in a controlled environment on their own premises.[182] Parties might also include generalized provisions of protection requiring parties to utilize "industry standard practices" to protect the data.[183] There is no catch-all provision for what is reasonable and what will satisfy ordinary care. The level of protection required will vary depending on the type of dispute and the information that is being transferred.

The reasonableness of a receiving party's data security measures depends on two vectors of proportionality: the value or complexity of the case and the value of the data involved. Smaller, low-value lawsuits have less at stake and will require less data security protection. Small cases may accordingly require less discovery, and the volume of data transferred may be smaller. By contrast, high-value, complex litigation may involve the transfer of millions of documents with significantly higher stakes. The sheer volume of data involved will naturally require more data security protection.

The value of the data itself will also affect the obligation owed by the receiving party. High-value, confidential data will require more protection than low-value data. A proprietary, trade secret document is high-value data that is deserving of greater protection than a routine business email. Due to the proportionality requirement set forth in Rule 26(b)(1), the ordinary care

181 Kessler et al., *supra* note 2, at 2.

182 *Id.* at 3.

183 *Id.*

standard effectively acts as a sliding scale based on the value of the litigation and the value and confidential nature of the data involved.[184]

Second, the ordinary care standard should require a reasonable response by the receiving party when there is a data breach. It has become increasingly common for protective orders to include provisions requiring receiving parties to take certain actions in response to a hack or breach.[185] Such provisions should require the receiving party to disclose to the producing party when a breach has occurred, as well as the extent of the breach, or even compel the requesting party to "investigate and remediate the effects of a breach."[186] No amount of security measures can prevent a data breach with one hundred percent success. It is not enough to simply put in place adequate security measures; the ordinary care standard should mandate that parties respond quickly and effectively to instances of data breach.

If the bailment standard of ordinary care is formally established, subsequent litigation will help to flesh out our understanding of ordinary care. If a party's ESI is hacked while in the possession of the receiving party and the receiving party fails to satisfy the ordinary care standard, the receiving party will be in violation of their discovery obligation. The judge tasked with ruling on the resulting motion will determine whether the security measures put in place by the receiving party were sufficient to satisfy ordinary care. With time, this new realm of discovery jurisprudence will further our understanding of what it means to have reasonable data security protections.

CONCLUSION

The solution to the rising threats to electronic data in the complex modern discovery process lies in the centuries-old principle of bailment. A bailment is simply defined as "the rightful possession of goods by one who is

184 *See* FED. R. CIV. P. 26(b)(1) (imposing a proportionality requirement on the scope of discovery that may be sought).

185 *See* THE SEDONA CONFERENCE, *supra* note 8, at 54 ("If a Receiving Party or Authorized Recipient discovers any loss of Confidential Material or Highly Confidential Material or a breach of security, including any actual or suspected unauthorized access, relating to another party's Confidential Material or Highly Confidential Material, the Receiving Party or Authorized Recipient shall: (1) promptly provide written notice to Disclosing Party of such breach; (2) investigate and make reasonable efforts to remediate the effects of the breach, and provide Disclosing Party with assurances reasonably satisfactory to Disclosing Party that such breach shall not recur; and (3) provide sufficient information about the breach that the Disclosing Party can reasonably ascertain the size and scope of the breach. The Receiving Party or Authorized Recipient agrees to cooperate with the Producing Party or law enforcement in investigating any such security incident. In any event, the Receiving Party or Authorized Recipient shall promptly take all necessary and appropriate corrective action to terminate the unauthorized access.").

186 Kessler et al., *supra* note 2, at 3.

not the owner."[187] As this Comment seeks to prove, the transfer of electronic information in the discovery process is a perfect fit for a bailment analysis. A receiving party obtains the electronic data of a producing party and possesses that intangible property for the course of litigation. When this separation of property and ownership occurs, a bailment is created.

The Supreme Court in *Seattle Times* missed an opportunity to provide clarity and certainty as to what duty is owed by a receiving party to protect the data of a producing party in discovery. In the distant wake of the *Seattle Times* decision, this Comment calls on courts to set a clear standard. The transfer of data in discovery to an opposing party is akin to a mutually beneficial bailment. Therefore, the applicable standard that should guide the exchange of ESI is ordinary care. Ordinary care is perhaps the best standard to fit the needs of the discovery world, as it mirrors the existing core principle of discovery: *reasonableness*. Protections that satisfy ordinary care are protections that are inherently reasonable.

If we assume that there is no common law, baseline standard of care owed by the receiving party, counsel for the producing party will effectively be required in every case to put provisions in a protective order binding the receiving party to take reasonable steps to protect transferred data. The production of data, without a protective order providing recourse for a data breach and an assurance that the data will be protected, would amount to data security negligence or malpractice on the part of counsel. Thus, the producing party will always demand contractual protections. It will be essential that "reasonable steps" is defined before any data is produced.

It is also in the best interest of the receiving party to delineate exactly what "reasonable steps" mean before they receive the data. If the receiving party fails to negotiate their obligations at the forefront of the case, they will be forced to guess as to what security measures will satisfy "reasonable steps." And, if a data breach occurs, the receiving party could be left without a set plan of action. The new system would provide a producing party with recourse in an instance of breach when a receiving party fails to satisfy reasonable steps.[188] In any event, it is in the best interests of both the producing and receiving parties to create a protective order that clearly sets forth what steps must be taken to protect the data and what to do in the event of a breach.

The resulting effects that a baseline standard of care will have on the protective order negotiation process cannot be understated. As the ordinary care standard becomes more robust over time, the efficiency of protective order negotiations will increase dramatically. A guiding standard will

187 WILLISTON & LORD, *supra* note 26, at § 53.1.

188 *Cf.* Schaller, *supra* note 66, at 266 (noting that "[v]iolating a protective order can lead to serious consequences").

introduce clarity in negotiations and make it easier for opposing parties to reach an agreement. An expedient and effective protective order negotiation process will both decrease overall discovery costs and ensure that litigants' data is protected by reasonable data security measures. As data security threats continue to rise in the modern discovery world, clients will rest easy knowing that their data is kept safe and that litigation costs are controlled.

* * * * *